при їх суміщенні з SEO (Search Engine Optimization). Пошуковий маркетинг і SEO-технології – це цілий комплекс заходів, який дозволяє збільшити відвідуваність сайтів. Хоча, пошуковий маркетинг сам по собі і не є рекламою, однак саме він дозволяє в рази підвищити її ефективність.

У завершенні з упевненістю можна констатувати, що технології розміщення реклами в соціальних мережах будуть розвиватися все більш високими темпами. Це дозволить автоматично показувати рекламу тільки для конкретної цільової аудиторії. Наприклад, жінці, якій показувалася реклама жіночого одягу, при зміні сімейного стану на «заміжня», стане показуватися також і реклама чоловічого одягу. Цей приклад заснований на тому, що жінки купують одяг своїм чоловікам частіше, ніж самі чоловіки. При цьому методики SMO і SMM є більш тонкими і більш дієвими інструментами, ніж традиційна реклама або навіть SEO-просування. Адже інформація в соціальних мережах поширюється з неймовірною швидкістю, і немає більш підходящої і ефективної реклами, ніж рекомендації друзів, знайомих або визнаних експертів у тій чи іншій області.

ІНФОРМАЦІЙНА БЕЗПЕКА

Опаленик Д.Я.
Науковий керівник – ***Гавриленко І.О., асистент***

Сучасну компанію неможливо уявити без інформаційних технологій. Будь-яка фірма, установа, підприємство містить величезну кількість комп'ютерних мереж. Бази даних, інформація про доходи, витрати, плани, конфіденційна інформація знаходяться всередині безлічі серверів. І, як показує практика, бувають викрадені.

Спроби зломів, апаратні вразливості портативних пристроїв, проблеми передачі конфіденційних даних через соціальні мережі, використання всесвітньої мережі, шифрування даних – тільки мала частина проблем, які відносяться до інформаційної безпеки.

Користувач не може постійно перебувати в офісі, працюючи за відносно захищеною машиною, яка унеможливлює спроби злому, тому користується портативними пристроями, які вже давно синхронізують з особистими і робочими даними. Портативні пристрої (смартфони і ноутбуки) в силу особливостей архітектури найчастіше піддаються атакам і перехопленнями даних.

Наведемо приклад однієї з поширених MITM-атак, коли зловмисник використовує Wi-Fi-маршрутизатор в якості інструменту перехоплення повідомлень. Зловмисник за GPS даними знає, в якому місці Ви

регулярно перебуваєте. Після невеликих маніпуляцій з громадською точкою доступу Wi-Fi в цьому місці, він починає свої роботи: налаштовує в своєму пристрої точку бездротового доступу, надає їй те ж ім'я, що і використовується в громадському місці з доступним Wi-Fi. В даному випадку створюється заміна роутера, що використовується, і заміна самої мережі. Або використовуються помилки в налаштуванні і захисті мережі, що дозволяють цілком легально перехоплювати сесії.

У опублікованому звіті компанії «SourceDNA» є інформація про те, що 256 iOS-додатків порушували політику конфіденційності «Apple», збираючи дані про e-mail адреси користувачів, встановлених програм, AppleID, серійні номери пристроїв та іншу особисту інформацію. Дослідники встановили, що 87,7% всіх Android-девайсів в світі схильні до хоча б однієї з 11 небезпечних критичних вразливостей.

Дослідники, що працюють в компанії «SR Labs» в області захисту даних, стверджують, що вада в протоколі USB дозволяє зловмисникам змінювати прошивку (внутрішню програму) пристроїв, які підключаються до комп'ютеру, і впроваджувати туди шкідливі модулі. Не слід здійснювати фінансові операції або передачу конфіденційних даних через соціальні мережі Wi-Fi і користуватися чужими USB-«флешками». Звичайний сучасний антивірус не зможе виявити «жучки» та інші хакерські прийоми. Найкращим виходом буде використання тільки перевірених пристроїв з перевіреними комп'ютерами.

Останнім часом зустрічається і варіант MITM-атаки «Людина-в-браузері». У цьому випадку зловмисник використовує один з декількох можливих методів для того, щоб занести шкідливий код, який працює всередині браузера, на комп'ютер жертви. Це програмне забезпечення потім непомітно записує всі дані, що передаються між браузером і різними сайтами, після чого відсилає отримані відомості зловмисникові. Є кілька ефективних засобів захисту від MITM-атак. Одним із способів захисту від такої атаки є використання стійкого шифрування між клієнтом і сервером. У такому випадку сервер може ідентифікувати себе за допомогою надання цифрового сертифікату, після чого між користувачем і сервером встановлюється шифрований канал для обміну конфіденційними даними. Але в цьому випадку виникає залежність від самого сервера і вибору методу шифрування. Прикладом програмного забезпечення для шифрування даних, якому не страшне перехоплення пакетів даних, є «TorMessenger», який нещодавно побачив світ.

Скільки б не з'являлося способів захисту даних – завжди з'являються нові способи їх крадіжки. Тому дуже важливо мати уявлення про загрози і мати в штаті співробітників, які спеціалізуються на інформаційної безпеці.